ARTICLE:

ELECTRONIC EVIDENCE AND THE CROATIAN CRIMINAL PROCEDURE ACT

By **Drazen Skrtic, Ph.D.**

The purpose of this article is to present the provisions on the temporary seizure of electronic data, the search and seizure of electronic devices, and to consider the rules to preserve electronic evidence under the provisions of the Croatian Criminal Procedure Act (CPA). An overview of the standard procedures for the seizure of electronic data and electronic devices and the searching and preservation of evidence from electronic devices is also covered. The article is based on the review and analysis of the provisions of the Croatian CPA, and decisions of the Croatian Constitutional court.

Introduction

In December 2008, the Croatian legislator adopted a new Criminal Procedure Act (CPA),[1] although it was amended before it entered in to force in September 2009.[2] The CPA has been amended on a number of occasions, and the last amendment was in 2013.[3] The intention of this new act is to provide for a modern system of rules of criminal procedure comparable to similar modern European procedure acts enacted in other countries. The CPA regulates two forms of criminal procedure: regular and summary proceedings. Summary proceedings cover the less serious criminal offences. The CPA provides for accelerated proceedings, direct transfer to a higher stage of proceedings, such as raising the indictment without an investigation, and the presentation of the evidence before raising the indictment. The CPA provides for a simpler procedure when the indictment refers to a minor criminal offence within the competence of a sole judge. The use of regular proceedings are proscribed in the case of the gravest criminal offences which are punishable by imprisonment[4] and long-term imprisonment,[5] which also includes the investigation and presentation of evidence before raising the indictment.

All charges are subject to preliminary court review. After confirming the indictment, the court conducts criminal proceedings and decides on what charges to press. The structure of the main trial has been retained, and it follows the traditional inquisitorial principle.

The crucial point of reform was a new definition of the position and role of State Prosecutors, and guarantees of protection from the unfounded intervention of rights and freedoms granted by the Constitution. The judge of investigation has replaced the controversial cumulative function of adjudication and investigation carried out in the person of the investigative judge. This is a new entity in the Croatian Criminal Procedure. The judge of investigation (and another body of the court) decides on interventions into fundamental rights, especially on measures of coercion, such as the preventive deprivation of freedom.

The State Attorney becomes the master[6] in the preliminary procedure, and he or she is in charge of the procedure of collecting data for the indictment. Under the terms of preliminary procedure, the State Attorney is the body in charge, and he or she conducts the criminal prosecution as the party representing the prosecution. The State Attorney examines the accused and the witnesses, and, in order to secure the presence of the accused, can order detention of the accused for 48 hours. The State Attorney may, through competent bodies, conduct a review of the operations of legal and natural persons, and seize monies, securities and documents.

The accused has rights established by law before and

1 *The Criminal Procedure Act was published in the Official Gazete Republic of Croatia No. 152/2008.*
2 *Act Amendming the Criminal Procedure Act was published in the Official Gazete Republic of Croatia No. 76/2009.*
3 *Act Amendming the Criminal Procedure Act was published in the Official Gazete Republic of Croatia No. 80/2011, 143/2012 and 56/2013.*
4 *Imprisonment may not be shorter than three months or longer than twenty years. Article 44(1) Penal Code.*
5 *Long- term imprisonment may not be shorter than twenty one years or longer than forty years. Article 46(1) Penal Code.*
6 *Latin – Dominus litis.*

during the criminal procedure, within the framework of collecting data on the criminal offence if this involves a temporary limitation on his or her constitutional rights and freedoms. Except in cases explicitly specified in the law, these rights may be the subject of intervention only on the basis of a court decision. The accused may file motions for actions from the moment they become aware that a criminal procedure is being conducted, until the completion of the procedure.

The investigation of criminal offences in the preliminary procedure has been organized in such a way as to allow for the efficient collection and effective processing of data, but the CPA also guarantees protection from unfounded interventions into the rights and freedoms of the accused, subjecting all such interventions to a preliminary decision by the court, or, when an action can be exceptionally ordered by a State Attorney, to a subsequent co-validation by the court.

The police focus their activity on detecting the criminal offence and on investigating criminal offences on the orders of the State Attorney. During the investigation, or in procedural actions prior to the raising of the indictment, specified police officers act as investigators. For specific criminal offences, other appropriately qualified agencies can also become involved as investigators if they are duly authorized. The State Attorney is responsible for conducting the investigation, and supervises the activities of the investigators, including the police officers as investigators.

The Criminal Procedure Act gives special attention to the regulation of the collection of evidence and the procedures to be followed. Electronic evidence must be obtained by applying the provisions of articles 257, 262 and 263 of the CPA.[7] The provisions regulate procedural activities connected with electronic evidence as follows:

a) the seizure of electronic devices and data carriers,

b) the searching electronic devices and data carriers, and

c) the seizure and preservation of data in electronic form.

Basic standards regulate the collection of electronic evidence for criminal proceedings by searching movable property; searching computers and devices connected with the computer; other devices for collecting, saving and the transfer of data; telephone, computer and other communications; data carriers; data that has been seized temporary, and data on devices used for collecting and transferring data, data carriers and subscription information that are in possession of a service provider.

The judge of investigation may, upon the written request (with a statement of reasons of the State Attorney), temporary restrict certain constitutional rights of the accused, including authorising surveillance and the interception of telephone conversations and other means of remote technical communication and interception, including the gathering and recording of electronic data.

The Police Duties and Powers Act[8] sets out the provisions relating to the obtaining of data which are generated or processed during electronic communications, including traffic and location data. Surveillance can be conducted against both legal entities and natural persons, including data identifying the subscriber or registered user.

An individual application was made to the Constitutional Court during 2009 and 2010 by a number of law firms and others[9] for a constitutional review of article 160 and part of article 579 of the Criminal Procedure Act.[10] The applicant argued that some of the provisions were inconsistent with the Constitution. The Constitutional Court issued two decisions, published on the same day in the Official Gazete. By decision one, the Constitutional Court decided not to accept the proposal to review the constitution.[11] By decision two, the Constitutional Court decided to accept the proposal to review the constitution,

7 *Article 331 CPA.*

8 *Zakon o policijskim poslovima i ovlastima (Unofficial translation into English – Police Duties and Powers Act), Official Gazete Republic of Croatia No. 76/2009.*

9 *Law Firm Nobilo and others from Zagreb, including Jasna Novak and Vi nja Dren ki Lasan, attorney at law from Zagreb, Zrinko Zrili , attorney at law from Zadar, Laura Valkovi attorney at law from Zagreb and Igor Rzaunek from Zagreb.*

10 *Article 38. (1) Every individual or legal person has the right to propose the institution of proceedings to review the constitutionality of the law and the legality and constitutionality of other regulations.(2) The Constitutional Court itself may decide to institute proceedings to review the constitutionality of the law and the review of constitutionality and legality of other regulations. (The Constitutional Act of the Constitutional Court of the Republic of Croatiapublished in the Official Gazete Republic of Croatia No. 49/2002).*

11 *Decision (Rješenje) No. U-I-448/2009 of 19 July 2012 – the decision was published in the Official Gazete Republic of Croatia No. 91/2012.*

initiated proceedings to review the constitutionality of the CPA, and repealed 43 provisions of the CPA.[12] Furthermore, the Constitutional Court decided that a number of provisions are inconsistent with the Constitution, but did not suspend those provisions, such as article 257 of the CPA (see below).[13] As a consequence, the last amendment to the CPA was made a few months later.[14]

The temporary seizure of electronic devices and the preservation of data in electronic form

Physical items that are seized temporarily are subject to the general provisions of the CPA regulating the seizure of objects. There are no provisions of a special nature that deal with the seizure of electronic devices, data in electronic format and subscription information.[15] The provisions on the temporary seizure of objects that are seized pursuant to the Penal Code, or which may be used to determine facts in proceedings, are covered by article 261 (paragraph 1) of the CPA. Article 261(1) also applies to data saved on computers and any devices that are connected to the computer, as well as on devices used for collecting and transferring data, data carriers and any subscription information that are in possession of the service provider.[16] The term 'computer and devices connected thereto' is a broad one in the CPA. It is used for electronic devices as well as devices connected to an electronic device, and also for electronic data holders. The CPA does not regulate the way in which an electronic device should be seized, or sets out the further steps that should be considered where an electronic device is seized, because investigating the content nor the method of preserving the data is prescribed in the provisions of the CPA.

Whoever is in possession of an object that is the subject of an investigation is bound to surrender them upon the request of the State Attorney, the investigator or the police authorities – who in turn are required to instruct the holder of the object of the consequences that will arise if they fail to comply with the request.[17]

Where a person fails to comply with the request to surrender the objects, even though there are no justified causes, they may be penalized by the investigating judge[18] upon a motion with a statement of reasons of the State Attorney.[19] Such coercive measures do not apply to the defendant or persons who are exempted from the duty to testify in accordance with the provisions of the CPA.[20] The police authorities are required to use such measures in accordance with provisions of the Police Duties and Powers Act.[21]

After the seizure and preservation of a device, the investigation of the device should be performed with the aim of establishing if there is any digital evidence connected to the criminal offence that is the subject of the investigation in accordance with provisions of the CPA. The methods use to preserve evidence are not prescribed.

The seizure and preservation of data in electronic form

Data must be handed over to the State Attorney upon his written request in a complete, original, legible and understandable format. It is for the State Attorney to stipulate in the request a period of time during which the data is to be given up. Where a person refuses[22] to provide the data, the matter may be pursued.[23]

12 *Article 55 (1) The Constitutional Court shall repeal a law, or some of its provisions, if it finds that it is not in accordance with the Constitution; or another regulation, or some of its provisions, if it finds that it is not in accordance with the Constitution and the law. (2) The repealed law or other regulation, or their repealed separate provisions, shall lose legal force on the day of publication of the Constitutional Court decision in the Official Gazette Narodne novine, unless the Constitutional Court sets another term. (3) The Constitutional Court may annul a regulation, or its separate provisions, taking into account all the circumstances important for the protection of constitutionality and legality, and especially bearing in mind how seriously it violates the Constitution or the law, and the interest of legal security:*
- if it violates the human rights and fundamental freedoms guaranteed by the Constitution,
- if, without grounds, it places some individuals, groups or associations in a more or a less privileged position. (The Constitutional Act of the Constitutional Court of the Republic of Croatia published in the Official Gazete Republic of Croatia No. 49/2002).

13 *Decision (Odluka) No. U-I-448/2009 of 19 July 2012 – the decision was published in the Official Gazete Republic of Croatia No. 91/2012.*

14 *Act Amendming the Criminal Procedure Act was published in the Official Gazete Republic of Croatia No.143/2012 and 56/13.*

15 *In Croatian legal theory there are two main types of provision, general and special. If there are conditions for use of special provisions, the general one is not used.*

16 *Article 263 (paragraph 1) CPA.*

17 *Article 261 (paragraph 2) CPA.*

18 *An investigating judge can issue a fine of up to HRK 50,000.00 (around 6.600 €), and if the person does not comply with the order, he may be sentenced to imprisonment until such time as the order is executed, but for no longer than one month; article 259 (paragraph 1) CPA.*

19 *Article 261 (paragraph 3) CPA.*

20 *Article 261 (paragraph 4) CPA.*

21 *Zakon o policijskim poslovima i ovlastima (Unofficial translation into English – Police Duties and Powers Act), Official Gazete Republic of Croatia No. 76/2009.*

22 *A person who fails to comply with the request to the State Attorney, even though there are no justified causes, may be penalized by the investigating judge upon a motion with a statement of reasons of the State Attorney.*

23 *Article 263 (paragraph 1) CPA. An investigating judge canissue a fine of up to HRK 50.000,00 (around 6.600 €), and if the person does not comply with the order, he may be sentenced to imprisonment until such time as the order is executed, but for no longer than one month; article 259 (paragraph 1) CPA.*

When authorised, the recording of data takes place in real time by the authority carrying out the action, and attention must be paid to the regulations regarding the obligation to observe confidentiality[24] during the acquisition, recording, and storing of data.[25] The methods used to preserve data are not proscribed. Although the provisions of the CPA do not prescribe the process of preserving the data in electronic form, nevertheless the hash value, or some other appropriate methods must be used to enable the subsequent checking of the identity and integrity of the preserved data.

The user of the computer and the service provider may file an appeal within twenty-four hours against the ruling of the investigating judge prescribing the measures. It is for the panel to decide on the appeal within three days. In any event, the appeal does not act to stay the execution of the ruling.[26]

Not all data that is seized can be retained. The investigating authorities must take into account the circumstances of the case. This means that data that is not related to the criminal offence for which the action is taken, may be recorded to an appropriate device, and then the data must be returned to the person, even prior to the conclusion of the proceedings.[27]

The CPA provides rules that regulate the retention of data that are seized. Upon a motion of the State Attorney, the judge of investigation may reach a decision on the protection and safekeeping of all electronic data. The length of time can be up to but no longer than six months. After this term data must be returned, unless:

1. They are related to committing the following criminal offences referred to in the Penal Code: breach of confidentiality, integrity and availability of electronic data, programs and systems (article 223), computer forgery (article 223a) and computer fraud (article 224a) of the Penal Code[28] respectively; where they are related to committing the criminal offences against a computer system, computer program and computer data, (Chapter XXV) of the Penal Code.

2. They are not used as evidence of a criminal offence for which proceedings are instituted.[29]

Searching electronic devices

Article 240 paragraph 1 of the CPA provides that the search must be undertaken in the manner stipulated in the Act and in other applicable regulations. The State Attorney, the investigator or the police authorities may carry out a search without a warrant when they carry out an on-site investigation of the site where a criminal offence was committed and which is subject to as public prosecution. This can occur immediately, or at least eight hours after the criminal offence was discovered. The provisions also apply to the search of movable property,[30] which includes the search of a computer and any devices that are connected to the computer; other devices for collecting, saving and transfer of data, telephone, computer and other communications, as well as data carriers.[31] This list is not closed, so other devices can be listed as an electronic device and will therefore be subject to the provisions of the additional articles. The investigation can be performed on the basis of the relevant provisions in the CPA without a court order or written consent given to the police, investigators or the State Attorney by the person using the computer or having access to the computer. The CPA does not provide for a search of a computer on the basis of the consent of the person who owns the computer.

The authority carrying out the search can request the person using the computer to provide access to the computer, device or any data carrier, and to give any necessary information for the fulfilment of the search objectives.[32] In addition, the authority carrying out the search can take measures to prevent the person using the computer from destroying or changing data.

The authority carrying out the search may order a professional assistant to undertake such measures.[33] As for the regulation, it is not necessary that an appropriately qualified police expert perform the search of electronic device. The legal term 'professional assistant' is broad enough to allow the police to employ the service of a digital evidence specialist from the private sector as and when they are needed.

Failure by the person who uses the computer or has access to the computer to cooperate or comply with the authority may be penalized by the investigating judge upon a motion with a statement of reasons of the State Attorney,[34] although coercion does not apply to the defendant.[35]

A record of each search must be made, signed by the person whose premises have been searched or who has

24 Articles 186 – 188 CPA.
25 Article 263 (paragraph 3) CPA.
26 Article 263 (paragraph 5) CPA.
27 Article 263 (paragraph 3) CPA.
28 Official Gazete Republic of Croatia No. 110/97, 27/98, 50/00, 129/00, 51/01, 111/03, 190/03, 105/04, 84/05, 71/06, 110/07, 152/08, 57/11 i 77/11.
29 Article 263 (paragraph 4) CPA.
30 Article 246 CPA.
31 Article 257(paragraph 2) CPA.
32 Article 257(paragraph 3) CPA.
33 Article 257(paragraph 2) CPA.
34 An investigating judge can issue a fine of up to HRK 50,000.00 (around 6.600 €), and if the person does not comply with the order, he may be sentenced to imprisonment until such time as the order is executed, but for no longer than one month; article 259 (paragraph 1) CPA.
35 Article 257(paragraph 3) CPA.

been searched and by the persons whose attendance at the search is obligatory. They must also be given a copy of the record.[36]

Searching without a warrant

The Constitutional Court has been required to consider whether it is possible under the constitution to search a computer without a warrant.[37] The Constitutional Court concluded that there was a breach of the Constitution, and committed the legislator to clearly prescribe the cases in which and for which offences are allowed to conduct a search without a warrant. The Constitutional Court is more restrained when it comes to the constitutionality of article 257 of the CPA, especially relating to the procedural guarantees relating to the search of computers, in that the Constitutional Court recommended a change to the CPA in accordance with the Constitution, and it reserved the right to re-examine the Constitution ex officio if and when such assessment is considered necessary.

It should be noted that the Constitutional Court did not considered compatibility of the provision in accordance with article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms, or the practice of the European Court of Human Rights in the case of *Malone v United Kingdom* (1985) 7 EHRR 14.

Surveillance and interception of conversations and interception of electronic data

If the investigation cannot be carried out in any other way, or for an investigation to be effective, or it can only be undertaken with great difficulty, the State Attorney can make an application to the judge of investigation to temporarily restrict certain constitutional rights of the citizen, including the surveillance and interception of telephone conversations and other means of remote technical communication; and the interception, gathering and recording of electronic data.[38] Any such application must include the available data on the person against whom the measures are to be applied, the facts justifying the necessity for applying the measures, and the term of their duration, which must be proportionate to the accomplishment of the objective, as well as the manner, the scope and the place of execution of the measure. It is for the police to execute the measures.

The data generated or processed during electronic communications

The Police Duties and Powers Act cover the relevant law.[39] A police officer may ask a telecommunication service provider to request the verification of the identity, frequency and duration of contact of relevant addresses and the physical location of any devices.[40] Such a request can only be made after the police officer has submitted a written request to the police authorities, such consent to be decided by the leader of the Criminal Police of the Ministry of Interior, or a person authorized by him.

There is an overlap between the provisions of the Police Duties and Powers Act and the provisions of CPA in terms of the powers to obtain subscriber information that are in possession of the service provider. The powers of a police officer are broad and include powers to obtain all data that are generated or processed during the electronic communications that are in possession of the service provider.

Conclusion

The new Croatian Criminal Procedure Act includes provisions on the seizure of electronic devices, the interception of electronic data, and the investigation and preservation of electronic data. The changes are only a modification of the traditional legal rules for obtaining classical forms of evidence. The legal regulations for obtaining electronic evidence is the start of the process of recognizing electronic evidence as factually equal to classical forms of evidence.

A significant problem relates to the regulation of the method of preservation of electronic evidence in non-volatile form. The rules for the temporary seizure of electronic devices and preservation of data in electronic form are inconsistent with the provisions of the Constitution and Constitutional Court. This has led the Constitutional Court to recommend that changes be made to the CPA in accordance with the Convention for the Protection of Human Rights and Fundamental Freedom and decisions of the European Court of Human Rights. It is highly probable that such changes will be made to the CPA.

The rules for obtaining data which are generated or processed during electronic communications that are in possession of the service provider are likely to be considered in the context of their agreement with the

36 *Article 248 (paragraph 1) CPA.*
37 *Constitutional Court Decision No. U-I-448/2009 of 19 July 2012. The decision was published in the Official Gazete Republic of Croatia No. 91/2012, para. 213.2.*
38 *Article 332 CPA.*
39 *Zakon o policijskim poslovima i ovlastima (Unofficial translation into English – Police Duties and Powers Act), Official Gazete Republic of Croatia No. 76/2009.*
40 *See Article 68 Zakona o policijskim poslovima i ovlastima (Unofficial translation into English – Police Duties and Powers Act), Official Gazete Republic of Croatia No. 76/2009.*

provisions of Constitution, article 8 of the Convention for the Protection of Human Rights and Fundamental Freedom and the practice of the European Court of Human Rights.

Drazen Skrtic, Ph.D., works at the Criminal Investigation Division, Karlovac Police Administration, Ministry of Interior, Croatia, and is also lecturer of law science at the Karlovac University of Applied Sciences.

Appendix

The provisions of the Croatian Criminal Procedure Act

d) Pretraga pokretne stvari i bankovnog sefa

Članak 257.

(1) Pretraga pokretnih stvari obuhvaća i pretragu računala i s njim povezanih uređaja, drugih uređaja koji služe prikupljanju, pohranjivanju i prijenosu podataka, telefonskim, računalnim i drugim komunikacijama i nositelja podataka. Na zahtjev tijela koje poduzima pretragu, osoba koja se koristi računalom ili ima pristup računalu ili drugom uređaju ili nositelju podataka, te davatelj telekomunikacijskih usluga, dužni su omogućiti pristup računalu, uređaju ili nositelju podataka, te dati potrebne obavijesti za nesmetanu uporabu i ostvarenje ciljeva pretrage.

(2) Po nalogu tijela koje poduzima pretragu, osoba koja se koristi računalom ili ima pristup računalu i drugim uređajima iz stavka 1. ovog članka, te davatelj telekomunikacijskih usluga, dužni su odmah poduzeti mjere kojima se sprječava uništenje ili mijenjanje podataka. Tijelo koje poduzima pretragu, može provedbu tih mjera naložiti stručnom pomoćniku.

(3) Osobu koja koristi računalo ili ima pristup računalu ili drugom uređaju ili nositelju podataka, te davatelj telekomunikacijskih usluga, a koji ne postupe prema stavku 1. i 2. ovog članka, premda za to ne postoje opravdani razlozi, sudac istrage može na prijedlog državnog odvjetnika kazniti prema odredbi članka 259. stavka 1. ovog Zakona. Odredba o kažnjavanju ne odnosi se na okrivljenika.

2. Privremeno oduzimanje predmeta

Članak 261.

(1) Predmeti koji se imaju oduzeti prema kaznenom zakonu, ili koji mogu poslužiti pri utvrđivanju činjenica u postupku, privremeno će se oduzeti i osigurati njihovo čuvanje.

(2) Tko drži takve predmete, dužan ih je predati na zahtjev državnog odvjetnika, istražitelja ili policije. Državni odvjetnik, istražitelj ili policija će držatelja predmeta upozoriti na posljedice koje proizlaze iz odbijanja postupanja po zahtjevu.

(3) Osobu koja ne postupi prema zahtjevu za predaju, premda za to ne postoje opravdani razlozi, sudac istrage može na obrazloženi prijedlog državnog odvjetnika kazniti prema članku 259. stavku 1. ovog Zakona.

(4) Mjere iz stavka 2. ovog članka, ne mogu se primijeniti prema okrivljeniku niti osobama koje su oslobođene dužnosti svjedočenja (članak 285.).

Članak 263.

(1) Odredbe članka 261. ovog Zakona odnose se i na podatke pohranjene u računalima i s njim povezanim uređajima, te uređajima koji služe prikupljanju i prijenosu podataka, nositelje podataka i na pretplatničke informacije kojima raspolaže davatelj usluga, osim kad je prema članku 262. ovog Zakona, privremeno oduzimanje predmeta zabranjeno.

(2) Podaci iz stavka 1. ovog članka, na pisani zahtjev državnog odvjetnika se moraju predati državnom odvjetniku u cjelovitom, izvornom, čitljivom i razumljivom obliku. Državni odvjetnik u zahtjevu određuje rok u kojemu se imaju predati podaci. U slučaju odbijanja predaje, može se postupiti prema članku 259. stavku 1. ovog Zakona.

(3) Podatke iz stavka 1. ovog članka, snimit će u realnom vremenu tijelo koje provodi radnju. Pri pribavljanju, snimanju, zaštiti i čuvanju podataka posebno će se voditi računa o propisima koji se odnose na čuvanje tajnosti određenih podataka (članak 186. do 188.). Prema okolnostima, podaci koji se ne odnose na kazneno djelo zbog kojega se postupa, a potrebni su osobi prema kojoj se provodi mjera, mogu se snimiti na odgovarajuće

sredstvo i vratiti toj osobi i prije okončanja postupka.

(4) Na prijedlog državnog odvjetnika sudac istrage može rješenjem odrediti zaštitu i čuvanje svih računalnih podataka iz stavka 1. ovog članka, dok je to potrebno, a najdulje šest mjeseci. Nakon toga računalni podaci će se vratiti osim:

1) ako nisu uključeni u počinjenje sljedećih kaznenih djela: povrede tajnosti, cjelovitosti i dostupnosti računalnih podataka, programa ili sustava (članak 223.), računalnog krivotvorenja (članak 223.a) i računalne prijevare (članak 224.a) iz Kaznenog zakona (»Narodne novine«, br. 110/97., 27/98., 50/00., 129/00., 51/01., 111/03., 190/03., 105/04., 84/05., 71/06., 110/07., 152/08., 57/11. i 77/11.) odnosno ako nisu uključeni u počinjenje kaznenih djela protiv računalnih sustava, programa i podataka (Glava XXV.) iz Kaznenog zakona,

2) ako nisu uključeni u počinjenje drugog kaznenog djela za koje se progoni po službenoj dužnosti počinjenog pomoću računalnog sustava,

3) ako ne služe kao dokaz za kazneno djelo za koje se vodi postupak.

(5) Protiv rješenja suca istrage kojim su određene mjere iz stavka 3. ovog članka, osoba koja se koristi računalom i osoba koja je davatelj usluga imaju pravo žalbe u roku od dvadeset četiri sata. O žalbi odlučuje vijeće u roku od tri dana. Žalba ne odgađa izvršenje rješenja.

Unofficial translation into English

d) Search of movable property and bank safe

Article 257

(1) The search of movable property also includes a search of a computer and devices connected to the computer, other devices for collecting, saving and transfer of data, telephone, computer and other communications, as well as data carriers. Upon the request of the authority carrying out the search, the person using the computer or having access to the computer or data carrier or the telecommunications service provider shall provide access to the computer, device or data carrier and give the information necessary to enable the objective of the search to be fulfilled.

(2) Upon the order of the authority carrying out the search, the person using the computer or having access to the computer and other devices referred to in paragraph 1 of this Article or the telecommunications service provider shall immediately undertake measures for preventing the destruction or the alteration of data. The authority carrying out the search may order a professional assistant to undertake such measures.

(3) The person using the computer or having access to the computer or other device or data carriers or the telecommunications service provider, who fails to comply with paragraphs 1 and 2 of this Article, even though there are no justifiable causes whatsoever, may be penalized by the investigating judge upon the motion of the State Attorney in accordance with provisions of Article 259 paragraph 1 of this Act. The penalty clause shall not apply to the defendant.

2. Temporary seizure of objects

Article 261

(1) Objects which have to be seized pursuant to the Penal Code or which may be used to determine facts in proceedings shall be seized temporarily and deposited for safekeeping.

(2) Whoever is in possession of such objects shall be bound to surrender them upon the request of the State Attorney, the investigator or the police authorities. The State Attorney, investigator or the police authorities shall warn the person in possession of the objects of the consequences that arise from refusing to comply with the request.

(3) A person who fails to comply with the request to surrender the objects, even though there are no justified causes, may be penalized by the investigating judge upon a motion with a statement of reasons of the State Attorney pursuant to Article 259 paragraph 1 of this Act.

(4) The measures referred to in paragraph 2 of this Article shall not apply either to the defendant or persons who are exempted from the duty to testify (Article 285).

Article 263

(1) The provisions of Article 261 of this Act also apply to data saved on the computer and devices connected thereto, as well as on devices used for collecting and transferring of data, data carriers and subscription information that are in possession of the service provider,

except in case when temporary seizure is prohibited pursuant to Article 262 of this Act.

(2) Data referred to in paragraph 1 of this Act must be handed over to the State Attorney upon his written request in a complete, original, legible and understandable format. The State Attorney shall stipulate a term for handing over of such data in his request. In case of refusal to surrender, it may be pursued in accordance with Article 259 paragraph 1 of this Act.

(3) Data referred to in paragraph 1 of this Act shall be recorded in real time by the authority carrying out the action. Attention shall be paid to regulations regarding the obligation to observe confidentiality (Articles 186 to 188) during the acquisition, recording, protecting and storing of data. In accordance with the circumstances, data not related to the criminal offence for which the action is taken, and are required by the person against which the measure is applied, may be recorded to an appropriate device and be returned to the person prior to the conclusion of the proceedings.

(4) Upon a motion of the State Attorney, the investigating judge may by a ruling decide on the protection and safekeeping of all electronic data from paragraph 1 of this Article, for as long as necessary, but not more that six months. After this term, the data shall be returned, unless:

1) they are related to committing the following criminal offences referred to in the Penal Code: breach of confidentiality, integrity and availability of electronic data, programs and systems (Article 223), computer forgery (Article 223a) and computer fraud (Article 224a) of the Penal Code – Official Gazete Republic of Croatia No. 110/97, 27/98, 50/00, 129/00, 51/01, 111/03, 190/03, 105/04, 84/05, 71/06, 110/07, 152/08, 57/11 i 77/11) respectively, they are related to committing the criminal offences against a computer system, computer program and computer data, (Chapter XXV) of the Penal Code,

2) they are related to committing another criminal offence which is subject of public prosecution, committed by using a computer system;

3) they are not used as evidence of a criminal offence for which proceedings are instituted.

(5) The user of the computer and the service provider may file an appeal within twenty-four hours against the ruling of the investigating judge prescribing the measures referred to in paragraph 3 of this Article. The panel shall decide on the appeal within three days. The appeal shall not stay the execution of the ruling.